17-23861

THE DISTRICT COURT OF MARYLAND FOR HOWARD COUNTY
SEARCH AND SEIZURE WARRANT

TO: ANY POLICE OFFICER OF COUNTY OF HOWARD

GREETINGS,

AND it appearing to me, from the Application and the Affidavit(s) attached to the Application and incorporated in it, that Probable Cause (reasonable grounds) exists to believe that on or in the following described cellular phones, computers, and electronic storage devices to wit:

CELLULAR PHONE(S), COMPUTER(S), ELECTRONIC STORAGE DEVICE(S) & DIGITAL CAMERA (WITH ANY REMOVABLE STORAGE):

1. External hard drive, serial number NA7EN786 (HCPD Evidence #5730-3)
2. Toshiba Satellite L15W-B1302 laptop, serial number 2F038030S (HCPD Evidence #5730-9)
3. Blue Fujifilm XP camera, serial number 4TB20697 (HCPD Evidence #5730-10)
4. SanDisk 8 gigabyte SD card (HCPD Evidence #5730-5)
5. Black tower computer in a Lian Li case (HCPD Evidence #5730-4)
6. Verizon Droid smartphone, Model XT1254 (HCPD Evidence #5730-13)
7. LG-VK810 (tablet computer / black in color) with an IMEI of 990002623202336 (HCPD Evidence #5730-14)
8. LG-VK810 with an IMEI number 990002624169759 (HCPD Evidence #5730-16)
9. Verizon Galaxy S7 smartphone IMEI number 355301077886706 (HCPD Evidence #4703-1)
10. Multiple USB, SD, and other memory drives (HCPD Evidence #5730-23)
11. HGST 500 GB Hard Drive (serial number 141215TM85G3G80BTNGS /HCPD Evidence #3714-1)

In the County of Howard, there is now being concealed certain property, to wit:

REFER TO ATTACHMENT A

which is/are contraband and/or evidence relating to the commission of the following crime(s), to wit:

These offenses are listed under the Annotated Code of Maryland under

CR 6-102(a):	**Arson First Degree**
CR 6-106:	**Burning with Intent to Defraud (Insurance)**

NOW THEREFORE YOU ARE COMMANDED, with the necessary and proper assistants to search forthwith the person(s), premises and/or motor vehicle(s) herein above described for the property specified, executing this warrant and making the search; and if property be found there, to seize it: leaving a copy of this warrant with an inventory of the property seized and returning this warrant with an inventory, if any, to me within ten days after execution of this warrant for further disposition in the manner provided by law.

GIVEN UNDER MY HAND THIS 23 DAY MARCH 2017.

JUDGE

17-23861

APPLICATION FOR SEARCH AND SEIZURE WARRANT

TO THE HONORABLE JUDGE Pamila J. P
OF THE DISTRICT COURT NUMBER 10 OF HOWARD COUNTY, MARYLAND

YOUR APPLICANT(S), the undersigned, being duly sworn, depose(s) and say(s) that she has/have reasonable grounds (probable cause) to believe that on or in the following described cellular phones, computers, and electronic storage devices to wit:

CELLULAR PHONE(s), COMPUTERS, AND ELECTRONIC STORAGE DEVICES:

1. External hard drive, serial number NA7EN786 (HCPD Evidence #5730-3)
2. Toshiba Satellite L15W-B1302 laptop, serial number 2F038030S (HCPD Evidence #5730-9)
3. Blue Fujifilm XP camera, serial number 4TB20697 (HCPD Evidence #5730-10)
4. SanDisk 8 gigabyte SD card (HCPD Evidence #5730-5)
5. Black tower computer in a Lian Li case (HCPD Evidence #5730-4)
6. Verizon Droid smartphone, Model XT1254 (HCPD Evidence #5730-13)
7. LG-VK810 (tablet computer / black in color) with an IMEI of 990002623202336 (HCPD Evidence #5730-14)
8. LG-VK810 with an IMEI number 990002624169759 (HCPD Evidence #5730-16)
9. Verizon Galaxy S7 smartphone IMEI number 355301077886706 (HCPD Evidence #4703-1)
10. Multiple USB, SD, and other memory drives (HCPD Evidence #5730-23)
11. HGST 500 GB Hard Drive (serial number 141215TM85G3G80BTNGS /HCPD Evidence #3714-1)

Your Affiant, Detective Marc Delbusso, can further identify said item(s). All items are currently being stored at the Howard County Police Department Property & Evidence Room.

In the County of Howard, there is now being concealed certain property, to wit:

REFER TO ATTACHMENT A

Which is contraband or evidence in relation to the commission of the following crime(s), to wit:

CR 6-102(a):	**Arson First Degree**
CR 6-106:	**Burning with Intent to Defraud (Insurance)**

AND YOUR APPLICANT further deposes and says that the facts which establish probable cause (reasonable grounds) for issuance of a Search and Seizure Warrant are set forth in the Affidavit of your affiant that is attached hereto and incorporated herein;

17-23861

WHEREFORE YOUR APPLICANT prays that a Search and Seizure Warrant be issued for the above described items.

Detective Marc Delbusso

SUBSCRIBED AND SWORN TO BEFORE ME THIS 23 DAY OF MARCH 2017.

JUDGE

AFFIDAVIT FOR A SEARCH AND SEIZURE WARRANT

Greetings,

Application is herewith made for a search and seizure warrant in that there is probable cause to believe that the laws relating to Arson and Burning with the Intent to Defraud (Insurance) prohibited under the Annotated Code of Maryland is being violated through the use of cellular phones, computers, and electronic storage devices.

IN SUPPORT OF THIS AFFIDAVIT

In support of this application and basis for probable cause, your Affiant is Detective Marc Delbusso of the Howard County Police Department, Criminal Investigations Bureau. Your Affiant has been a member of the Criminal Investigation Division since August 2004. Affiant Delbusso is a duly sworn Officer; Certified by the Maryland Police Training Commission. Your Affiant has been a duly constituted member of the Howard County Police Department since July of 1995 who has served in a past assignment as a Patrol Officer under the Operations Command Division. Your Affiant has attended and successfully completed: (1) a twenty-six week Law Enforcement Academy conducted by the Howard County Police Department. During the academy, your Affiant received detailed instruction in topics, which include (but not to limited to) the following: Theft, Fraud, Controlled Dangerous Substances, Assault, Robbery, Interview and Interrogation, Constitutional Law, Criminal Law and Preparation of Search and Seizure Warrants, (2)Howard County Police Department Criminal Investigators School (1997), (3) Surveillance Techniques for Covert Police Officers (Pa. 2001), (4) Domestic Terrorism / Extremist Groups Training (Baltimore Field Office / F.B.I. 2001), (5) Electronic Surveillance Training (U.S. Dept. of Defense 2002), (7) Howard County Police Department Special Weapons And Tactics School (2003), (8) Johns Hopkins University: Identity Theft & Computer Crime Investigation (2004), (9) Maryland State Police: Computer Crime Investigation (2005), (10) Federal Bureau of Investigation & National White Collar Crime Center: Internet Crime Seminar (Arizona 2005), (11) Public Safety Institute (University of Florida) Investigation of Fraudulent Document School (2006), (12) Howard County Police Department Tactical Section: Tactical Ballistic Breacher School (2006), (13) John E. Reid School of Interview and Interrogation (2008), (14) Forgery Detection & Handwriting Identification (Instructor Joseph Lucas / Forensic Document Examiner / Sponsored By the Hartford County Sheriff's Office, Maryland), (15) Identity Theft (2008 Maryland Public Safety Training Commission), (15) Auto Theft Investigator Course (Sponsored by the Baltimore Regional Auto Theft Task Force / October 26-30, 2009 / Loyola University, MD), (16) Odometer & Title Fraud (Sponsored by The National Highway Traffic Safety Administration and the Maryland Motor Vehicle Administration / November 18-19, 2009 / College Park, MD), (17) Street Racing Fraud & Theft (Mid-Atlantic Auto Theft Investigators Association / April 8, 2010 / Loyola Graduate Center / Columbia, MD) (18) Auto Arson Training (Maryland Insurance Administration, The Maryland/DC Anti-Car Theft Committee & The Anne Arundel County Fire Department / September 8, 2011), (19) Search Warrant Mini-Camp 2011 (Maryland Police Training Commission & The Office of the Prince George's County State's Attorney / January 21, 2011 / Fraternal Order of Police Lodge #89 Upper Marlboro, MD), (20) Auto Arson Training / Maryland Insurance Administration, The Maryland/DC Anti-Car Theft Committee & The Anne Arundel County Fire Department / September 8, 2011), (21) Motor Vehicle Identification & Auto Theft Symposium / January 23-27, 2012 / Miami-Dade Public Safety Training Institute / Miami, Fl).

AFFIDAVIT FOR A SEARCH AND SEIZURE WARRANT

Your Affiant Delbusso has had the opportunity to make arrests of individuals for thefts, theft schemes and fraud. Your Affiant Delbusso has assisted other officers in making arrests of individuals for multiple violations of law as well as executing numerous search and seizure warrants for evidence of crimes. Your Affiant is a graduate of the Indiana University of Pennsylvania with a B.A. Degree in Criminology and has completed coursework towards a Masters Degree in Criminal Justice from Aspen University.

The following circumstances are offered as probable cause:

On March 10, 2017 at 2355 hours, Howard County 911 received multiple calls reporting a fire at 11910 Emerald Court, Ellicott City, Howard County, Maryland 21042. Responding firefighters encountered a single family home fully engulfed in flames. After an exhaustive investigation, the cause of the fire was undetermined. The structure was destroyed and uninhabitable. Michael Fitzpatrick was identified as the homeowner. This information was verified through Maryland Department of Assessments & Taxation (Real Property).

Michael Fitzpatrick arrived at the scene and was interviewed by investigators. Fitzpatrick was utilizing crutches and had a cast on his left leg. He advised he recently had a scheduled surgery on his foot (Thursday March 9, 2017).

Detective Delbusso obtained the following information from the interview:

- Fitzpatrick left the residence on 3/9/17 at approximately 0930 hours for his scheduled surgery
- After the surgery (3/9/17) he was picked up by his fiancé, Linda Rabinovich
- Due to the surgery, Fitzpatrick had planned to stay at Rabinovich's residence approximately 1 week
- Fitzpatrick denied having any major problems with his home but did advise the circuit breaker would "trip" in his home office
- He thought it may have to do with the use of his printer and stated it would happen approximately once a week
- Fitzpatrick owns three dogs and had his ex-wife (Allison Fitzpatrick) care for two of them
- The other dog was brought to Rabinovich's residence
- He had a Nest Thermostat (WiFi) and Nest Smoke Detector (WiFi) installed in his home (11910 Emerald Court, Ellicott City, Maryland)
- He voluntarily showed investigators his cell phone screen which displayed the open Nest Application
- Fitzpatrick handed his phone to investigators and advised "He really didn't know how to work it"
- The Nest Application displayed a calendar type format (March 1-10)
- Investigators noted a message displayed on March 10 which read: "Offline" When the "Offline" message was accessed, Investigators noted the system went "Offline" at approximately 1900 hours (3/10/2017)
- Fitzpatrick voluntarily drew a sketch of the interior of his home. This sketch included his home office, where he advised his printer would sometimes cause the breaker to trip
- He advised the printer was plugged into a power strip which was plugged into a wall outlet

- Fitzpatrick specifically stated the circuit breaker would "trip" rather than the power strip
- Det. Delbusso questioned Fitzpatrick on why the power strip wouldn't "trip"
- Fitzpatrick advised he didn't know and re-affirmed it was the circuit breaker that would periodically "trip"
- Fitzpatrick stated "What about my cars?" (referring to his 2011 BMX X5 and 2017 Chevrolet Camaro) * Fitzpatrick never asked or commented regarding the status of any other items in his home

On 3/12/17 Det. Delbusso contacted Fitzpatrick at Rabinovich's home. At that time, Fitzpatrick gave investigators written consent to access his trailers and detached garage. While speaking with Fitzpatrick, he stated "Was it electrical?" Det. Delbusso asked Fitzpatrick to show him his Nest (WiFi Thermostat) application on his cell phone. Fitzpatrick voluntarily complied. Det. Delbusso noticed there was no longer a "Offline" message for 3/10/17.

Later that evening (3/12/17), Det. Delbusso located a computer (tower unit), printer, and computer monitor, located in the detached garage (pole-barn / located to the rear of the property / 11910 Emerald Ct. Ellicott City, MD). These items were not setup (connected/receiving power), they were located on the cement floor to the rear of the building. These items were photographed.

On 3/13/17 Linda Rabinovich (Fitzpatrick's fiancé) contacted Det. Delbusso. She advised she was very concerned about items she recently discovered in her home belonging to Michael Fitzpatrick. Rabinovich provided the following information to Det. Delbusso:

- She was cleaning out a closet (located in computer room / home office)
- She doesn't regularly use the closet in question
- She located additional clothing belonging to Fitzpatrick
- This surprised her because Fitzpatrick was only supposed to stay at her home for about a week
- She grew more suspicious and looked around the office where Fitzpatrick had set up his work computer for the week
- Rabinovich photographed a 'Spreadsheet style" document on Fitzpatrick's computer
- This spreadsheet displayed some of Fitzpatrick's financial liabilities (outstanding bills)
- Based on the information on the spreadsheet, Fitzpatrick owes approximately $1,000,000 to various creditors
- She located sentimental items in a black folder with Fitzpatrick's initials on the front
- The folder contained sentimental pictures of Fitzpatrick's children (pictures appeared to be approximately 8-10 years old) and home- made holiday cards from his children (approximately 8-10 years old)
- Rabinovich located a bill from the Internal Revenue Service (IRS) revealing Fitzpatrick owed over $118,000
- She also located multiple computers/related equipment (Tower unit, Tablet, Portable External-Hard Drive, Tower Unit Hard Drive, SD cards)

On 3/14/17, Detectives from the Howard County Police Criminal Investigations Section responded to [redacted] Pikesville, MD 21208) per her request. Detective's seized a external hard drive (serial NA7EN786 / HCPD Evidence #5730-3), Toshiba Satellite laptop L15W-B1302 (serial number 2F038030S / HCPD Evidence #5730-9), Blue Fujifilm XP camera (serial number 4TB20697 / HCPD Evidence #5730-10), Sandisk 8 gigabyte SD card (HCPD Evidence #5730-5), black tower computer in a Lian Li case (HCPD Evidence #5730-4), Multiple USB, SD, and other memory drives (HCPD Evidence #3714-1).

The items were secured at HCPD Southern District Police Station in preparation for a search & seizure warrant.

- After the fire (3/16/17), Fitzpatrick told Rabinovich he hid money at her residence
- Fitzpatrick eventually advised he hid $50,000 in cash (US Currency) in her sweater drawer (later located & photographed by Rabinovich)
- Rabinovich added, on 3/11/17 she witnessed Fitzpatrick receive a phone call from Allstate Insurance regarding the fire insurance claim
- Rabinovich described Fitzpatrick as having "fake tears" when speaking with the Allstate representative
- She felt Fitzpatrick was acting distraught just for the Allstate phone call
- Fitzpatrick immediately reverted back to his normal/calm demeanor once the phone call ended
- Rabinovich advised she now feels Fitzpatrick's previous (last three months) actions are suspicious: Removing his home television and taking it to Rabinovich's home (Although her television is functioning properly), Removing a large amount of bakeware/cookware from his home and giving it to Rabinovich (Although she has no need for additional bakeware/cookware), removing his home wireless speaker sound system and installing it over Linda Rabinovich's home
- Rabinovich did not request any of the above listed items from Fitzpatrick

Subsequent to seizing the items from Rabinovich's home, on 3/14/17 Michael Fitzpatrick was arrested for illegally possessing a regulated firearm & ammunition. These items were located/seized (Search & Seizure Warrant signed by Honorable Judge McCrone) by Det. Delbusso on 3/14/2017. Search incident to arrest of Michael Fitzpatrick, Detectives seized (2) two cell phones and (2) two computer tablets. A Verizon Galaxy S7 smartphone IMEI number 355301077886706 was seized from his person (HCPD Evidence #4703-1). A Verizon Droid smartphone, Model XT1254 (HCPD Evidence #5730-13), LG-VK810 (Computer tablet - IMEI of 990002623202336 / HCPD Evidence #5730-14), and a LG-VK810 (Computer tablet - IMEI number 990002624169759 / HCPD Evidence #5730-16) were seized from the interior of Michael Fitzpatrick's Dodge Truck (MD Registration 3CG4117). These items were secured at HCPD Northern & Southern District Police Stations in preparation for a search and seizure warrant.

During a post-Miranda interview, Fitzpatrick provided the following information to Det. Delbusso:

- Regarding what personal items he keeps at Rabinovich's residence – Response: A shaving kit and some clothes
- Why he had his children's pictures and hand-made cards – Response: "I take them everywhere I go….Even on vacation."
- Det. Delbusso asked Fitzpatrick to describe his current financial situation (Personal & Landscaping Business / RMF Inc.)
- Fitzpatrick advised "good" and made no indication he or his business was in financial distress
- When confronted with the $118,000 IRS tax bill, he first alluded the bill may be fraudulent
- He later acknowledged he hasn't filed tax returns for the past three (3) years
- Fitzpatrick advised he owns a single family home in Virginia (Smith Mountain Lake area)
- Fitzpatrick stated he has a large attached garage at his home in Virginia
- Fitzpatrick advised he has two (2) Acura NSX Race Cars, which he normally stores in the attached (lower) two car garage at 11910 Emerald Ct. Ellicott City, MD - (Estimated value of Acura's $150,000)

- Fitzpatrick admitted to relocating the Acura NSX Race Cars to his detached garage (lower portion of his property (11910 Emerald Court, Ellicott City, MD)
- He acknowledged the race cars were moved out of his garage(s) a few days prior to the house fire
- Det. Delbusso asked if he had moved any of his property to his home in Virginia
- Fitzpatrick advised he doesn't go to his Virginia home often in winter
- He stated me made two (2) trips to that location (over the past two months)
- He stated he moved his "outdoor" porch furniture to Virginia because it was stored outdoors here at 11910 Emerald Ct. Ellicott City, MD

- He moved his leather couch, originally stored in the basement at Emerald Ct. (MD) to his Virginia home

On 3/19/17 investigators interviewed Fitzpatrick's son, Ryan Fitzpatrick, regarding items which were at the house before the fire occurred. He was shown the picture of the aforementioned computer, monitor and printer which were located by police in his father's detached garage (3/12/17). Ryan Fitzpatrick advised the computer tower belonged to him and was in his bedroom at 19110 Emerald Ct. Ellicott City, MD. He stated the last time he observed his computer in his bedroom was on 3/10/17 (Wednesday, two days prior to the house fire). He also advised the monitor and printer belong in his father's home office (11910 Emerald Ct. Ellicott City, MD). He also advised investigators the older couch from the Virginia home had been placed in the basement on Wednesday (3/8/17 – two days prior to the fire / replacing the more expensive leather couch). Ryan Fitzpatrick stated he never experienced any electrical problems regarding the use of the printer in his father's home office.

During a follow up interview with Linda Rabinovich, she advised Michael Fitzpatrick was very proficient with technology (computers, etc.). She stated her "Jaw Dropped" when Det. Delbusso advised Fitzpatrick stated he "Really didn't know how to work his Nest (WiFi Termostat)". She stated (as a couple) they went on approximately (15) fifteen vacations over the past (18) eighteen months. Linda Rabinovich stated she never observed Fitzpatrick take his children's sentimental pictures and hand-made cards on their vacations. She advised he always kept those items in his home office (located at 11910 Emerald Court, Ellicott City, MD). Approximately (3) weeks prior to the house fire, Rabinovich observed missing/removed ceiling tiles and "wires" were hanging down from the drop ceiling (basement / 11910 Emerald Ct. Ellicott City, MD)

Michael Fitzpatrick's home located in Virginia has been identified as: 300 Indian Ridge Drive, Moneta, VA 24121. On or about 3/15/17, local law enforcement investigators assisting with the investigation contacted neighbors of Michael Fitzpatrick. A neighbor advised Fitzpatrick doesn't normally stay at the home (Virginia) in the winter. This neighbor advised he has recently observed Michael Fitzpatrick make trips to the home (past few weeks). The neighbor advised he observed "trucks and trailers" at the residence. The neighbor stated this behavior was "Not Normal".

Your Affiant knows through his training, knowledge, and experience that suspect(s) will commit arson to collect on insurance claims. Suspects will remove items of value; both financial and sentimental (computers, electronics, expensive vehicles, family photographs, home-made cards from family). Suspect(s) will also commit "Arson for Profit" to alleviate personal/commercial debt. Suspect(s) will also "stage" the scene (House) and replace expensive furnishings with older less expensive ones.

Your affiant knows that perpetrators of crimes often password-protect their phones and/or internal SIM cards. This action is intended to hide their criminal activity and to prevent the collection of evidence being stored if their device is ever intercepted. Your affiant knows that for iPhones in particular, an encrypted plist file storing the device's password is saved in a known and specific location on a computer that it has been synced and backed up to and that a search of the owner's computer can further reveal that password.

Your affiant knows that cellular phones have the technology and capability to send and receive instant messages from a computer. Cell phones also have the capability to send and receive text messages between other cell phones. Many cell phones come standard with still photography and video recording functionality. They can take and receive pictures and videos created by the device or others. In addition, these pictures, videos, instant and text messages can be saved onto a cell phone device and its internal memory card.

Your affiant knows that perpetrators of a crime often email, text or instant message others in the hours or minutes building up to the crime to inaudibly plan their course of action. Perpetrators of a crime often use their cell phone to aid them in committing their crime such as placing phone calls to potential victims. Perpetrators of a crime often take pictures or make a video record of them committing such crimes using their cell phone. This is to later reflect upon and glorify what they did. Your affiant know that the perpetrators of such crimes would often display the pictures or videos from these crimes, or in other words post their work on social networks such as Facebook, Twitter, Skype, Youtube, "Worldstarhiphop", Instagram and Tumblr etc., to show-off what they've done and to receive attention from admirers.

Your affiant believes that information relevant to this investigation in the form of text messages, voice mail messages, instant messages, email, call logs, historic cell tower records, contact lists, web browsing history, IP and/or wireless connections, passwords, calendar, pictures, audio files and videos are still currently on the aforementioned cell phone(s). "Smart" cellular devices are programmed to capture location data by storing latitude and longitude coordinates and hexadecimal MAC addresses. The status of all of the above listed data is historical in nature and archived within specific areas of the device. The retrieval of data from these devices could support or contradict information and/or evidence obtained during the course of this investigation and could produce inculpatory and/or exculpatory evidence.

Your affiant know based on their training, knowledge and experience that searching cell phones for criminal evidence is a highly technical process requiring a properly controlled environment. The detailed examination of data contained within a cellular phones memory requires individuals who specialize in special applications designed for examination of cellular phones. Nonetheless, it is difficult to know before a search which expert is qualified to analyze the cellular phone and its data. In any event, cell phone data search protocols are exacting scientific procedures designed to locate and protect the integrity of the evidence and to recover even hidden, erased, password-protected or encrypted files. Because cell phone evidence is vulnerable to inadvertent or intentional modification and destruction, a controlled environment will be necessary to complete an accurate analysis; which in most cases take a considerable amount of time to complete.

Your affiant knows that cell phones are used much like a computer and act much like a computer when it accesses, uses and stores information. Therefore, a cell phone could be considered to be a computer and have been recognized by courts to be such in determining how to retrieve and analyze information from it.

Your affiant is aware through training, knowledge and experience that trained, qualified forensic examiners can retrieve communications sent through cell phones, and that this data is static in nature when not being used, manipulated and powered off. Your affiant further knows that since the cell phone(s) were never opened, powered-on, disturbed or manipulated, that data originally believed to be in the phone(s) when first petitioned the Court for a search warrant for the analysis of them, are still

there, unchanged, unaltered, undamaged and not destroyed.
Your affiant also knows that files or remnants of such files can be recovered months or even years after they have been downloaded onto a cell phone if the device is kept in a forensically sound manner, which is turned off, packaged in accordance with best methods and practices and undisturbed. Electronic data files downloaded to a cell phone can be stored for years if kept in these conditions and its data recoverable as it was last left. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools rendering staleness moot for the purposes of recovering evidence from these devices.
Lastly, your affiant knows that when a person "deletes" a file, the data contained in the file does not actually disappear; rather, that data remains in the file system of that device until it is overwritten by new data through further usage. Therefore, data or deleted data may reside within cell phones for long periods before they are overwritten if remained in a sterile environment.
Based upon the above information your affiant believes that probable cause exists that all cell phones seized pursuant to this search warrant contain evidence related to this investigation, Furthermore, your affiant asks that this search and seizure warrant allow for the seizure and specialized search of all phones seized pursuant to an Arson and Burning with Intent to Defraud (Insurance).

PROPERTY / INFORMATION TO BE SEIZED:

1. All Text messages
2. All Application "App" Data and Content
3. All Phonebook contacts
4. All Assigned phone numbers
5. All Call history
6. All Images
7. All IP address information
8. All plists, SQL files
9. All Videos
10. All Audio files
11. All Voice memos
12. All GPS files
13. All Call alerts
14. All Calendar360
15. All Emails
16. All Installed applications
17. All Web search history

Based on Your Affiant knowledge, training and experience, Your Affiant knows that computer files or remnants of such files, such as a picture or videos, can be recovered months or even years after they have been placed on a media card, or a computer. Electronic files downloaded to any storage device can be stored for years at little or no cost. Even when such files have been deleted, there is a chance that they can be recovered months or years later using readily-available forensic tools.

Your Affiant knows through his training, knowledge, and experience, that the digital media card's storage process is much like the process for digital storage on a computer hard drive, or other removable media, such as a "thumb drive."

Your Affiant knows that searching and seizing information from computers, or removable

media storage devices, often requires that police officers seize most or all electronic storage devices to be searched later by a qualified computer forensics technician in a laboratory or other controlled environment. This is true because of the following:

THE VOLUME OF EVIDENCE : Computer storage devices (like a removable media card) can store the equivalent of thousands and thousands of pages of text, hundreds of images; and the capacity of these types of storage devices is ever increasing.

TECHNICAL REQUIREMENTS : Searching computer systems, such as a removable storage device, for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. In any event, however, data search protocols are exacting, scientific procedures designed to protect the integrity of the evidence and to recover even "hidden", erased, deleted, compressed, password-protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (either from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment may be necessary to complete an accurate analysis.

In light of these concerns, your affiant, Your Affiant, hereby requests the Court's permission to seize the removable media storage devices that is believed to contain some or all of the evidence described in the Attachment of the Warrant, and to conduct an off-site search and examination for the evidence described.

Searching the suspect's removable digital storage media system for the evidence described in the Attachment may require a range of data analysis techniques. In some cases, it is possible for police officers to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials
that may be commingled with criminal evidence. For example, computer forensic technicians may be able to execute a "keyword" search that searches through the files stored in a computer for special words that are likely to appear only in the materials covered by a Warrant.

Suspects are known to purposely mislabel or hide files and directories; encode communications to avoid using keyword; attempt to delete files to evade detection; or take other steps designed to frustrate law enforcement searches for information. These steps may require computer forensic technicians to conduct more extensive searches, such as scanning areas of the disks not allocated to listed files, or opening every file and scanning its contents briefly to determine whether it falls within the scope of the Warrant. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in the Attachment.

Today, computers are also capable of disguising or hiding data to hinder or to prohibit its detection. Computers are capable of encrypting data so as to make it un-retrievable by the average computer user. The Alcohol, Tobacco, Firearms and Explosives Computer Crime Forensics Division is in possession of computer software that will assist in breaking some forms of encryption but the use of such software can be time-consuming, depending upon the amount of data stored and the complexity of the encryptions.

Attempting to decrypt data is an extremely time and equipment intensive process, requiring a laboratory environment to be done effectively. Some users will purposefully rename files with otherwise innocuous file names to deter curiosity seekers and others. Similarly, computer users may also "booby-trap" their computers or password-protect their computer systems in an attempt to hide their activities and prevent the collection of incriminating evidence.

Computers and the Internet have revolutionized the way individuals research, communicate, through email and social media, post blogs, letters, and diaries of personal nature. People with mental illness and thoughts of suicide; may search view and participant in websites, blogs, forums or communicate their thoughts and feelings with individuals and groups without having physical interaction or identities known to include family and friends. Your affiant knows that using a computer on the internet creates historical logs of internet activity to include content, people, topics, product searches, favorite URL (website addresses), websites visited, images and videos downloaded using an internet browser such as; Mozilla FireFox, Google Chrome, Internet Explorer and Apple Safari. These historical logs and internet activity are stored on the computer's hard drive, which is located inside of a computer, automatically in operating system created files called "temporary internet files". Additionally, applications and software programs also stored on the computer's hard drive, may create historical logs of activity to include: social media posts, messages, and locations to websites like "Twitter", "Facebook," and "Instagram" or "digital communications" in the form of email, instant and multimedia messaging, and VOIP using programs such as "Skype," "SnapChat," "KIK," "ChatON", "AIM" and many others.

With this knowledge and basis for probable cause, your Affiant Detective Delbusso, prays that a Search and Seizure Warrant be issued authorizing him, with the necessary and proper assistance to:

A. Search the cellular telephones for all incoming / outgoing telephone calls, all video / picture images, all contact numbers, names and addresses stored in the telephone, email addresses, all text messages, all application "App" data and content, all phonebook contacts, all assigned phone numbers, all call history, all Images, all IP address information, all plists, SQL files, all videos, all audio files, all voice memos, all GPS files, all call alerts, all Calendar360, all Emails, all Installed applications, all Web search history.
B. View, photograph, seize, examine and process any and all electronic data processing and storage devices, computers systems, including central processing units, internal and peripheral storage devices such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, optical readers and scanning devices, CD ROM drives and compact disks and related hardware, operating logs, software and operating instructions, operating manuals, computer materials, software and programs used to communicate with other terminals via telephone or other means, and any computer modems, monitors, printers, etc. that may have been used while engaging in the crime(s) of Arson and Burning with Intent to Defraud (Insurance).

Detective Marc Delbusso

SUBSCRIBED AND SWORN TO BEFORE ME THIS 23 DAY OF MARCH 2017.

JUDGE

APPLICATION FOR SEARCH AND SEIZURE WARRANT
ATTACHMENT A

PROPERTY TO BE SEIZED:

1. Cell phone and computer-related items subject to search and seizure are as follows:

- External hard drive, serial number NA7EN786 (HCPD Evidence #5730-3)
- Toshiba Satellite L15W-B1302 laptop, serial number 2F038030S (HCPD Evidence #5730-9)
- Blue Fujifilm XP camera, serial number 4TB20697 (HCPD Evidence #5730-10)
- SanDisk 8 gigabyte SD card (HCPD Evidence #5730-5)
- Black tower computer in a Lian Li case (HCPD Evidence #5730-4)
- Verizon Droid smartphone, Model XT1254 (HCPD Evidence #5730-13)
- LG-VK810 (tablet computer / black in color) with an IMEI of 990002623202336 (HCPD Evidence #5730-14)
- LG-VK810 with an IMEI number 990002624169759 (HCPD Evidence #5730-16)
- Verizon Galaxy S7 smartphone IMEI number 355301077886706 (HCPD Evidence #4703-1)
- Multiple USB, SD, and other memory drives (HCPD Evidence #5730-23)
- HGST 500 GB Hard Drive (serial number 141215TM85G3G80BTNGS /HCPD Evidence #3714-1)

To effectuate the search and to the extent necessary retrieve responsive documents which may be stored electronically, the following items will be seized as needed:

a. Hardware:

Computer hardware consisting of all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computerized impulses or data. Hardware includes, but is not limited to, any data processing devices (such as central processing units, memory typewriters, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices (such as fixed disks, disk drives and diskettes, tape drivers and tapes, optical storage devices, transistor-like binary devices, and other memory storage devices); cellular telephones (including personal digital assistants (PDAs), smart phones, and tablets); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communication devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or part that can be used to restrict access to computer hardware (such as physical keys and locks).

b. Documentation:

Computer-related documentation consisting of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use the computer hardware, software, or other related items.

c. Software:

Computer software is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communication programs.

d. Passwords and Data Security Devices:

Computer passwords and any other data security devices are designed to restrict access or hide computer software, documentation or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

The terms "records," "documents," and "materials" include all of the following items of evidence in whatever form and by whatever means such records, documents, or materials, their drafts, or their modifications may have been created and stored, including but not limited to: any handmade form (such as writing or drawing with any implement on any surface, directly or indirectly); any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); any mechanical form (such as phonograph records, printing, or typing); and any electrical, electronic, or magnetic form (such as tape recordings, cassettes, compact discs or any information on an electronic or magnetic storage device, such as floppy discs, compact discs, hard disks or drives, CD-ROMs, optical discs, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drivers, cellular telephones, personal digital assistants (PDAs), smart phones, tablets, or electronic notebooks, as well as printouts or readouts from any magnetic storage device.

Det. [signature]

Detective Marc Delbusso

SUBSCRIBED AND SWORN TO BEFORE ME THIS 3 DAY OF MARCH 2017

[signature]

JUDGE